



DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID DoD-2022-OS-0051]

Privacy Act of 1974; System of Records

AGENCY: Department of Defense (DoD).

ACTION: Notice of a new system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the DoD is establishing a new Department-wide system of records titled, “Defense Advisory Committees,” DoD-0011. This system of records covers DoD’s maintenance of records about proposed, appointed, and prior members of the DoD’s Federal Advisory Committees, to include subcommittees, which are or not subject to the Federal Advisory Committee Act (FACA). Individuals may be appointed to serve on an advisory committee as a regular government employee, as a special government employee, or as a representative member when directed by statute. These records include information on individuals who applied to be on a committee/subcommittee, were considered for, are currently serving on, and/or had previously served on a committee/subcommittee.

DATES: This system of records is effective upon publication; however, comments on the Routine Uses will be accepted on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]. The Routine Uses are effective at the close of the comment period.

ADDRESSES: You may submit comments, identified by docket number and title, by any of the following methods:

* Federal Rulemaking Portal: <https://www.regulations.gov>. Follow the instructions for submitting comments.

* Mail: Department of Defense, Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, Regulatory Directorate, 4800 Mark Center Drive, Attn:

Mailbox 24, Suite 08D09, Alexandria, VA 22350-1700.

Instructions: All submissions received must include the agency name and docket number for this *Federal Register* document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at <https://www.regulations.gov> as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Ms. Rahwa Keleta, Privacy and Civil Liberties Division, Directorate for Privacy, Civil Liberties and Freedom of Information, Office of the Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency, Department of Defense, 4800 Mark Center Drive, Mailbox #24, Suite 08D09, Alexandria, VA 22350-1700; OSD.DPCLTD@mail.mil; (703) 571-0070.

SUPPLEMENTARY INFORMATION:

I. Background

DoD is establishing the Defense Advisory Committees, DoD-0011, as a DoD-wide Privacy Act system of records. A DoD-wide system of records notice (SORN) supports multiple DoD paper or electronic recordkeeping systems operated by more than one DoD component that maintain the same kind of information about individuals for the same purpose. Establishment of DoD-wide SORNs helps DoD standardize the rules governing the collection, maintenance, use, and sharing of personal information in key areas across the enterprise. DoD-wide SORNs also reduce duplicative and overlapping SORNs published by separate DoD components. The creation of DoD-wide SORNs is expected to make locating relevant SORNs easier for DoD personnel and the public, and create efficiencies in the operation of the DoD privacy program.

The FACA is a Federal law that governs the establishment, operation, and termination of advisory committees. The FACA ensures the public's knowledge of and an opportunity to participate in meetings between Federal agencies and groups the agency either established or manages and controls for the purpose of obtaining group advice and recommendations regarding

the agency's operations or activities. The FACA requires the charter of such groups, meetings announced in advance and open to the public, and the availability of work products to the public.

This system of records will support relevant and appropriate offices and personnel, to include the DoD Advisory Committee Management Officer /who collects and preserves the required personally identifiable information necessary for proposed, appointed, and prior DoD advisory committee/subcommittee members. The system of records will consist of both electronic and paper records and will be used DoD-wide, for approved personnel, to maintain records of Federal government employees and other persons who participate in DoD-sponsored Federal advisory committees/subcommittees. The collection and maintenance of this information will enable DoD to maintain a list of members of its various Federal advisory committees/subcommittees subject to the FACA. This system of records will provide DoD with information on committee/subcommittee membership balance, qualifications, functions, and required reporting. This information is especially pertinent to selection of who will serve as an advisory committee/subcommittee member.

DoD SORNs have been published in the *Federal Register* and are available from the address in FOR FURTHER INFORMATION CONTACT or at the Defense Privacy, Civil Liberties, and Freedom of Information Directorate website at <https://dpcl.d.defense.gov>.

II. Privacy Act

Under the Privacy Act, a "system of records" is a group of records under the control of an agency from which information is retrieved by the name of an individual or by some identifying number, symbol, or other identifying particular assigned to the individual. In the Privacy Act, an individual is defined as a U.S. citizen or lawful permanent resident.

In accordance with 5 U.S.C. 552a(r) and Office of Management and Budget (OMB) Circular No. A-108, DoD has provided a report of this system of records to the OMB and to Congress.

Dated: May 6, 2022.

Aaron T. Siegel,

Alternate OSD Federal Register

Liaison Officer, Department of Defense.

SYSTEM NAME AND NUMBER: Defense Advisory Committees, DoD-0011.

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Department of Defense (Department or DoD), located at Defense Pentagon, Washington, DC 20301-1950, and other Department installations, offices, or mission locations. Information may also be stored within a government-certified cloud, implemented and overseen by the Department's Chief Information Officer (CIO), 6000 Defense Pentagon, Washington, DC 20301-6000.

SYSTEM MANAGER(S): The system managers are as follows:

A. Advisory Committee Management Officer, Office of the Director of Administration and Management, 1950 Defense Pentagon, Washington, DC 20301-1950.

B. The Designated Federal Officer (DFO), serves as the system manager for individual DoD federal advisory committees. The contact information for the current DFO for each DoD committee can be found on <https://www.facadatabase.gov/>.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 10 U.S.C. 113, Secretary of Defense; 5 U.S.C., Appendix, as amended, Federal Advisory Committee Act (FACA); 14 U.S.C. 632, Functions and powers vested in the Commandant; 19 U.S.C. 2071 note, Establishment of Service; Commissioner; Appointment; 41 CFR 102.3.5 through 102.3.185, Federal Advisory Committee Management; DoD Instruction 5105.04, Department of Defense Federal Advisory Committee Management Program; and E.O. 9397, Numbering System For Federal Accounts Relating To Individual Persons as amended;.

PURPOSE(S) OF THE SYSTEM:

A. To collect and maintain information on DoD past, present, and proposed advisory committee/subcommittee members subject to the FACA.

B. To identify the most qualified applicant and ensure a balanced advisory committee/subcommittee.

C. To support studies, findings, and recommendations to the Secretary of Defense and the Deputy Secretary of Defense, through the advisory committee's sponsor, as identified in the committee's Charter.

D. To conduct required oversight and compliance over DoD advisory committee/subcommittee appointments and actions.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Any individual who:

A. Applied to be on a committee/subcommittee and was considered for a committee/subcommittee appointment.

B. Currently serves on a committee/subcommittee.

C. Previously served on a committee/subcommittee.

Note: Individuals may be appointed to serve on an advisory committee pursuant to 41 CFR 102-3.130(a) as a regular government employee, pursuant to 5 U.S.C. 3109 as a special government employee, or as a representative member when directed by statute.

CATEGORIES OF RECORDS IN THE SYSTEM: The following categories of records may be collected:

A. Personal information to include: name; DoD ID numbers; place and date of birth; gender; ethnicity; biographical information; addresses; e-mail address; telephone number(s); marital status; military service; education/degrees/certifications; and registration in professional societies.

B. Employment information to include: employer; title; work experience; professional awards; performance records; publications authored; DoD advisory committee/subcommittee membership and other board and committee memberships such as contractors or private organizations.

C. Any other information collected to determine if an individual is qualified to serve on a committee/subcommittee.

RECORD SOURCE CATEGORIES: Records and information stored in this system of records are obtained from the individuals listed in Categories of Individuals, above.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING

CATEGORIES OF USERS AND PURPOSES OF SUCH USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, all or a portion of the records or information contained herein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government when necessary to accomplish an agency function related to this system of records.

B. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.

C. To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.

D. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.

E. To the National Archives and Records Administration (NARA) for the purpose of records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

F. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

G. To appropriate agencies, entities, and persons when (1) the DoD suspects or confirms a breach of the system of records; (2) the DoD determined as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

H. To another Federal agency or Federal entity, when the DoD determines information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal government, or national security, resulting from a suspected or confirmed breach.

I. To another Federal, State or local agency for the purpose of comparing to the agency's system of records or to non-Federal records, in coordination with an Office of Inspector General in conducting an audit, investigation, inspection, evaluation, or some other review as authorized by the Inspector General Act.

J. To such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.

K. To the General Services Administration for the purpose of keeping Congress and the public informed about the existence, membership, and activities of advisory committees as authorized by the Federal Advisory Committee Act.

L. To the Executive Office of the President, the Office of Management and Budget, or other agencies for coordination on advisory committee member selection.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records may be stored electronically or on paper in secure facilities in a locked drawer behind a locked door. Electronic records may be stored locally on digital media; in agency-owned cloud environments; or in vendor Cloud Service Offerings certified under the Federal Risk and Authorization Management Program (FedRAMP).

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records may be retrieved by individual's name or other personal identifier.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

The records of DoD Committees/Subcommittees are managed in accordance with General Record Schedule 6.2, Federal Advisory Committee Records, or other approved agency records disposition schedule.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: DoD safeguards records in this system of records according to applicable rules, policies, and procedures, including all applicable DoD automated systems security and access policies. DoD policies require the use of controls to minimize the risk of compromise of personally identifiable information (PII) in paper and electronic form and to enforce access by those with a need to know and with appropriate clearances. Additionally, DoD has established security audit and accountability policies and procedures which support the safeguarding of PII and detection of potential PII incidents. DoD routinely employs safeguards such as the following to information systems and paper recordkeeping systems: Multifactor log-in authentication including Common Access Card (CAC) authentication and password; physical token as required; physical and technological access controls governing access to data; network encryption to protect data transmitted over the network; disk encryption securing disks storing data; key management services to safeguard encryption keys; masking of sensitive data as practicable; mandatory

information assurance and privacy training for individuals who will have access; identification, marking, and safeguarding of PII; physical access safeguards including multifactor identification physical access controls, detection and electronic alert systems for access to servers and other network infrastructure; and electronic intrusion detection systems in DoD facilities.

RECORD ACCESS PROCEDURES: Individuals seeking access to their records should follow the procedures in 32 CFR part 310. Individuals should address written inquiries to the DoD component with oversight of the records, as the component has Privacy Act responsibilities concerning access, amendment, and disclosure of the records within this system of records. The public may identify the contact information for the appropriate DoD office through the following website: www.FOIA.gov. Signed written requests should contain the name and number of this system of records notice along with the full name, current address, and email address of the individual. In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the appropriate format:

If executed outside the United States: “I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature).”

If executed within the United States, its territories, possessions, or commonwealths: “I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature).”

CONTESTING RECORD PROCEDURES: Individuals seeking to amend or correct the content of records about them should follow the procedures in 32 CFR part 310.

NOTIFICATION PROCEDURES: Individuals seeking to determine whether information about themselves is contained in this system of records should follow the instructions for Record Access Procedures above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: None.

